inadequate change control practices for such a long period. The controls established should include:

- Change management function should have the only authority to update and change the production library

- Programmers can check-out programs and JCL for purposes of making changes and testing

- Access to test library entries should be restricted to only those programmers with a reason to access those programs

Finding 118 - DOT does not have a disaster recovery plan.

The department has no documented disaster recovery plan.

Recommendation - Develop a disaster recovery plan immediately.

MIS should develop a disaster recovery plan for both its SIPS mainframe applications and also those running on the AS/400s within the department. DOT should also contact the Department of Public Instruction to discuss the potential use of the same IBM AS/400 for its hot site as will be used as DPI's hot site.

Finding 119 - DOT's management of telecommunications is fragmented.

The MIS telecommunications group is responsible for the following data communication areas:

- Installing data communication equipment, e.g., terminals or multiplexers, but no voice equipment

- Preparing VTAM generation procedures

- Planning

- Trouble shooting

Voice communication is not the responsibility of MIS. It is handled by each individual division (DOH, DMV, and General Services). The department has not integrated the support of voice and data communications.

Recommendation - Consolidate the responsibilities for voice and data communications in the MIS Department.

This will enable DOT to plan and support both voice and data needs with better service and more cost-effectiveness.

Finding 120 - Current application system security practices are obsolete.

Like all other State agencies, DOT has what is called Level 1 security for all systems running at SIPS (i.e., RACF ID and PASSWORD protection). All regions are under control of RACF.

Most of the transaction level security is now performed by CICS. As of CICS Release 3.2, CICS will no longer support these security functions. IBM will be expecting all security to be handled by RACF. This will be a major impact on DOT. Furthermore, many of the systems used within DOT have internal application system level security (e.g., terminal IDs).

All new systems are being developed using RACF and DB/2 security facilities.

Recommendation - Study requirements to upgrade security processing to RACF for current systems.

MIS should study the changes required both to remove CICS and application level security from the current systems and to implement RACF level security. MIS should then implement a program to migrate to RACF level security.

Even though DOT plans to replace the older production systems with new systems that will be designed to use RACF security features, the modernization process may take eight to ten years to complete. DOT cannot wait that long to move to the newer versions of CICS, and should not continue to live with systems utilizing application level security.

Finding 121 - DOT handles production control of its application systems differently from all other agencies running at SIPS.

There is no production control function in DOT, while every other agency that processes at SIPS has one. When DOT gave up its mainframe computer and operators to SIPS, it was agreed that SIPS would handle all production control activities for DOT. This has apparently worked well since the operators at SIPS running the DOT applications were former DOT staff. They know the systems and how to run them. The production systems require significant manual intervention and the former DOT operators understand these needs of the production systems.

MIS recognizes that the new systems, though heavily on-line, will still have major batch components, and DOT will need to decide how these new systems will be handled for production control.

Recommendation - DOT And SIPS should assess production control for DOT systems.

DOT and SIPS should study and evaluate whether SIPS should continue to perform the production control function for DOT. If SIPS is to continue to perform this function, there should be written justification to continue to manage DOT's production systems differently from all other State systems. It is not known at this time what the most cost-effective approach is for providing the production control function to the State agencies. This study should answer that question.

EMPLOYMENT SECURITY COMMISSION

The mission of the Employment Security Commission (ESC) is to promote the economic well-being of the citizens of North Carolina by aiding in the stabilization and growth of the State's economy through facilitating the operation of the labor market. ESC has determined that utilizing information technology, especially in the area of self-service, is a primary method to more cost-effectively deliver the services of the commission and to achieve its mission and objectives.

The Division of Information Systems (DIS), reporting to the Assistant Commissioner for Administrative Services, is responsible for the planning and delivery of information technology services for the commission.

Since 1985, ESC has pursued an aggressive automation strategy that has resulted in the automation of such functions as:

- On-line recording of claimant information at each local office, and payment of unemployment insurance benefits from the central office bi-weekly

- On-line access to job service information for both North Carolina employers and job applicants

- Efficient gathering of quarterly wage data and accurate processing of employer tax reports and monies

- Use of voice response systems to process and validate unemployment benefit processing

Some of the information technology initiatives now being undertaken by DIS are:

- Common Intake--a comprehensive applicant data base that is designed to eliminate duplication in data gathering

- Automated Adjustments--the automation of the manual adjustments required to track and report employer indebtedness to the Commission

- Adjudication and Appeals--automated updating of the North Carolina Benefit Payment System

The data processing needs of ESC are currently supported by the IBM mainframe at SIPS. ESC contributes close to one third of all the processing done at SIPS.

In summary, ESC has one of the State's most progressive information resource management functions. It has been leading the State in automating mission critical functions, which has resulted in improved services to the State's citizens at a reduced cost.

The major findings and recommendations concerning information technology and telecommunications within ESC follow.

Finding 122 - ESC does not have a comprehensive life cycle methodology.

ESC's standard life cycle methodology (LCM) contains most of the critical elements required of a good system development methodology. It contains a definition of the major life cycle phases, major tasks and sub-tasks within each life cycle phase, key considerations for each task within a phase, deliverables at the task level, and the participants at each task level. The standard states that each new phase must be approved prior to initiation, but does not state by whom. It acknowledges the need for deviations and waivers, which can be given by the Director of DIS. It also acknowledges the need to collapse phases for small projects; however, there is no guidance provided. It requires that a project notebook be maintained and changes to the project be logged and managed.

The LCM is weak in that it does not address the areas of structured analysis, design, and programming techniques, nor the use of automated CASE tools. It also does not address the evaluation and selection of application software packages. Also, some of the life cycle task descriptions are superficial. Furthermore, although it identifies the documents which need to be produced, the LCM does not provide an outline for those deliverables.

Recommendation - Incorporate structured techniques and CASE tools into the life cycle methodology.

ESC should either update its current life cycle methodology or consider purchasing one that contains all the necessary components. The new LCM should address structured techniques, CASE and other tools, and software package evaluation and selection.
ESC should give special attention to Andersen's Method/1 and FOUNDATION since they contain all the components missing in ESC's current LCM, and since most of the other large State agencies, including SIPS, have decided to standardize on this methodology and set of CASE tools. Further, State standardization on a single LCM and set of CASE tools will make sharing resources and hiring DIS staff within the State easier.

Finding 123 - DIS does not have a current consolidated set of policies, procedures, and standards.

The current DIS policies, procedures, and standards in ESC are a combination of old outdated binders and a loose collection of more current memos and documents addressing various topics (e.g., JCL standards and security). There is no single consolidated manual in which to locate the department's DIS policies, procedures, and standards.

DIS is currently updating all its standards and plans to place them on-line for access by all ESC, including field offices. At the time of the performance audit, DIS had already prepared a new table of contents for its revised standards. It had also collected related material into a loose collection of folders that it is currently using as its reference library for standards. Many of the chapters identified in the new table of contents do not exist as folders, and finding information that does exist is very difficult and time consuming. Many of the available standards are really procedures (e.g., computer access security procedures).

DIS intends to let a contract to complete the outline of the standards manual and then develop the full set of standards.

Recommendation - Complete the new standards manual expeditiously.

ESC should complete the development of a consolidated policies, procedures, and standards manual as soon as practical and place it on-line for easy access. This effort should be given higher priority and the resources made available to complete the effort in a timely manner. The life cycle management methodology discussed in the earlier section should be referenced in the new manual.

Finding 124 - DIS reports too low in the ESC organization.

DIS reports directly to one of the four line organizations it must support, Administrative Services. There has been discussion within ESC to move the function to a staff position reporting to the Chairman, ESC.

Recommendation - DIS should report higher in the ESC organization.

DIS should be reorganized as a staff function reporting to the Chairman, ESC. This should facilitate DIS's providing better support to all the line organizations within ESC, and allow greater visibility to its potential programmatic clients.

Finding 125 - There is inadequate control over dissemination of computer output.

The DIS Production Control section does not currently maintain a log of personnel authorized to receive output distribution. This is a matter of security over physical reports of information that is just as important as the automated security provided over data files.

Recommendation - Production control should maintain a distribution control list.

There should be a list of authorized users who can accept and pick up output. There should also be an output log that identifies who picked up computer output and when.

Finding 126 - DIS lacks the necessary policies and procedures for running its computer operations.

There is a lack of adequate controls and procedures in DIS's computer operations area. The following were noted:

- There are no run books. The policy has been that all documentation for a run is incorporated as JCL comments, which is an acceptable approach. However, in some cases the documentation is out of date. Also, only a few Check Point/Restart points and controls are documented.

- All jobs are manually initiated. There is no usage of SIPS' automated scheduler software package, ZEKE.

- There are no retention policies or procedures concerning tapes. The Computer Operations Manager stated that he will be looking for an appropriate tape management system.

The Computer Operations Manager had only been in his position for 90 days at the time of the performance audit and was working very hard to address the issues in his area. Significant efforts to improve the computer operations area were noted.

Recommendation - Develop the necessary policies, procedures, and controls for the computer operations area.

DIS should continue to follow the direction that has been set by the new manager of its computer operations area. This should include developing necessary policies, procedures, and controls to effectively manage that operation. DIS needs to make available the resources and time for these procedures to be developed and implemented.

In addition, training in automated tools like SIPS's automated scheduler, ZEKE, and a tape management system should be made available to the department's operators.

Finding 127 - ESC does not have an effective Help Desk operation supporting its users.

ESC has a Help Desk function, but it has been primarily involved with terminal/line problems. It has been staffed with a telecommunications person, and very few application problems come through the Help Desk. There is no automated problem tracking system in use, but problem reports are logged and tracked manually.

The Computer Operations Manager's concept is to make this the one contact point for all users concerning any system problem. He has recently obtained a new position that will be used to receive all calls, dispatch those calls to the appropriate person for resolution, and close out incidents.

Recommendation - Implement an effective Help Desk to support all ESC users.

ESC should follow through with the Help Desk concept put forth by the Computer Operations Manager. The new dispatcher function should receive all help and problem-related user calls that enter the department. The dispatcher should log the call into an automated problem tracking system. The tracking system should be capable of recording such information as who initiated the call, when the call was received, type of problem encountered, who the problem was referred to for resolution, recommended resolution, and the date the problem was closed. The dispatcher should route the request for help or problem resolution to the appropriate individual in the telecommunications, operations, security, or application area.

DIS management should periodically run reports off the Problem Tracking System to identify problems not resolved in a timely manner and trends in recurring problems.

Finding 128 - DIS does not have consolidated project level plans that can be monitored and reviewed by management.

There is no consolidated set of plans for the systems work underway in ESC. DIS requires that individual project plans be maintained in the project notebooks. However, no notebook reviewed contained a comprehensive set of detail plans, although some contained work breakdown structures related to project plans. Furthermore, the plans were not consistent in their content or level of detail.

Recommendation - Define and maintain consistent detailed project plans.

The plans should include a work breakdown structure (appropriate for the size and complexity of the project), planned start date, actual start date, planned completion date, actual completion date, original estimated person hours, actual person hours. The plan should be maintained on an automated system with reports generated at least weekly.

NORTH CAROLINA GENERAL ASSEMBLY

As stated in the 1991-1993 Biennium Budget, the mission of the General Assembly is to enact general and local laws promoting the best interests of the State and the people of North Carolina. The General Assembly is comprised of 170 members, 50 Senators and 120 Representatives, who are elected every two years. The members meet in a long session and a short session during each biennium. The long sessions occur in odd-numbered years and usually run from January through July. The short sessions, which are primarily for updating the second year of the biennium budget, occur in the even-numbered years and usually run from mid-May through June.

The General Assembly has centralized legislative services that are governed by the Legislative Services Commission (LSC), which has staffing and administrative oversight of the operations of the General Assembly. The LSC administers six divisions, including the Legislative Automated Systems Division (LASD).

LASD is responsible for providing the automated application system, office automation, and computer operations support needed by the North Carolina General Assembly. Support goes to two types of users:

- Member offices, which include both the General Assembly members and their administrative/clerical support

- Staff, which includes the attorneys, fiscal specialists, etc., supporting the work of the General Assembly

The computer applications required by these users include:

- Word processing

- Electronic mail

- Bill typing

- Bill status

- Access to the State Information Processing Services computer

- Data base management and spreadsheets

In addition, LASD supports such applications as the General Assembly's payroll and accounting system and the redistricting application.

To support these applications, LASD maintains and operates a number of Digital Equipment Corporation (DEC) mini-computers and micro-computers:

- VAX 8650, 8700, and 6000/410 configured in a VAX Cluster
- VAX 11/730 (supporting payroll)
- 2 MicroVAXs
- VAX 3100
- VAXstation II

Because of the nature of the General Assembly, the work placed on the computer systems is very seasonal, with most of the work coming when the General Assembly is in session.

The major findings and recommendations concerning information technology and telecommunications within the Legislative Automated Systems Division of the North Carolina General Assembly follow.

Finding 129 - Policies and procedures in LASD are not complete.

The automated systems policies provided by LASD only address access to the computer, applications, and data. The automated system procedures address authorization for access to the computer and internal data center operational procedures (e.g., back-up). No policies or procedures exist in areas such as:

- System change requests
- Testing
- Change management
- Problem management
- Training
- New equipment requests
- New software requests
- Fraud, waste or abuse
- Job promotions

- Security, in general

The Manager of LASD commented that end-users did not take training seriously, and many have not participated in regularly scheduled training courses. Nevertheless, no written policies exist concerning user training.

Recommendation - Develop a complete set of IRM policies and procedures.

LASD should develop a comprehensive and complete set of policies and procedures governing the use, access, security, integrity, and application of information technology. It should be disseminated both within the IRM function and throughout the General Assembly.

For an organization to make the most effective use of its automated resources, there need to be guidelines and procedures governing the use and access to these resources. The need for such well documented policies and procedures is especially critical in an organization like the General Assembly where there is a high turnover of administrative/clerical personnel and members themselves.

Findings 130 - LASD does not have a complete set of standards for its automated systems.

The standards used in LASD identify an in-house developed life cycle methodology that appears to be consistently followed. This is a very high level methodology that addresses what has to be performed, but not how, and does not address the specific content of the deliverables of each life cycle phase. Given the few systems developed in the division and the relatively small size of most systems that are developed, the level of detail of the methodology appears to be adequate.

However, the standards should still describe the contents of the deliverable(s) to be produced during each stage of the life cycle, major milestone review points, responsibilities of individuals, and the techniques to be used (e.g., structured design) in developing the systems.

LASD provided a transmittal memo addressing the standard programming languages, data bases, 4th generation languages, etc. used in the division. These standards are not written in any internal division standards manual or memo. The documentation that was provided did not contain any written evidence of a number of standards that should exist in a data center, namely:

- Data naming standards

- Program naming standards

- Data set naming standards

- Programming language coding standards (e.g., structured code)
- Testing standards
- Quality assurance standards

Recommendation - Develop a comprehensive standards manual.

LASD should develop a single document that contains all the required standards necessary to properly manage and maintain the data center. These standards should be applied to both internal and vendor developed systems and, where practical, to software packages procured.

LASD should also expand its life cycle methodology in include the descriptions of the contents of the deliverable(s) to be produced at the end of each life cycle phase, the technique to be used during each life cycle phase, responsibilities of individuals, and the interim milestone review points where approval is required to continue.

Finding 131 - Project plans for system development and maintenance projects are generally at too high a level.

Project plans were reviewed for the projects that will be addressed in each of the major application areas. These plans were in sufficient detail to identify the end product to be produced, but not to support accurate estimation of the time and effort to complete the job nor to support proper management and control of the project. The project plans did not include estimated hours of effort at any level. Projects are assigned to the responsible LASD staff, and when a completion date is established, the Division Manager expects the projects to be completed. The process has been working, but its effectiveness is highly dependent on quality staff and relatively straightforward, moderate sized projects.

Recommendation - Standardize on more detailed project plans.

LASD should institute the practice of developing detailed work breakdown structures, interim milestone dates, and resource estimates for all projects. Application development and maintenance projects require detailed work breakdown structures and estimates of person-hours to ensure that the project can be completed on time without placing undue pressure on the development staff. Detailed project plans will help prevent staff from being over- or under-committed to project work, and will provide the manager a better mechanism for monitoring project progress.

Finding 132 - Problem recording and tracking is not a centralized function and is performed manually.

LASD provided samples of problem logs. The completion of the problem reports is the responsibility of the individual who receives the call or the person the call is routed to. Problem reporting forms were on the desks of many of the staff.

The staff reported that they complete these forms at the time a user calls in with issues. However, there is no problem report numbering system or tracking system to ensure that a problem is completely resolved in a timely manner. Since the system is not automated, it is also more difficult to assess trends.

Recommendation - Institute a central automated problem reporting and tracking system.

All problem calls should come to a single individual or dispatcher who will assess the general nature of the problem. Each problem should be immediately entered in the tracking system along with the date and name of the requestor, given an identification number, and assigned to an analyst for detailed analysis and resolution. Once the nature of the problem has been assessed, an estimated date for completion should be entered by the analyst. Upon completion of the problem resolution, the completion date with the actions taken should be entered into the system and the problem closed. The final action is to contact the user who called in or reported the problem, and inform him of the resolution.

Finding 133 - LASD does not have a complete disaster recovery plan.

LASD's current Disaster Recovery Plan document is an excellent starting point for an effective disaster recovery plan. Some of the strengths of the current plan include:

- Risks are clearly identified and evaluated by their likelihood and impact on the data center
- Application systems and programs are prioritized by their criticality to the mission of the General Assembly, and recovery time frames are established for each
- Responsible individuals and their telephone numbers are documented, as well as the numbers of critical vendors
- Configuration detail and inventories exist for hardware, telecommunications, and software
- The disaster recovery plan (for one disaster scenario) is tested each year

Although the overall plan is a good starting point, several items are not adequately addressed and reduce the usefulness of the plan:

- The disaster scenario that is addressed is far from the worst possible case the General Assembly could face. The scenario involves the elimination of one of the multiple VAX processors on the network, and the recovery plan is the reinitialization of the missing application (e.g., payroll) on another still functioning VAX.

  A far worse disaster scenario, and one that is possible in the Raleigh region, is a tornado destroying both the Legislative Building and the Office Building at the same time. Several years ago a tornado touched down only a few miles from the SIPS data center. A disaster of this magnitude would require significant additional planning, preparation, and effort to recover from than the scenario addressed in the disaster recovery plan.

- Back-up tapes are stored in either the Legislative Building or Legislative Office Building. The back-up tapes from the VAX Cluster in the Legislative Office Building are sent to a vault in the Legislative Building, while the back-up tapes from the Legislative VAXs are sent to the VAX Cluster Computer Room in the Legislative Office Building. Not only could a major disaster destroy the computer in both buildings, but it could also destroy all back-up tapes.

Recommendation - Strengthen the disaster recovery plan.

LASD needs to develop a disaster recovery plan for a more comprehensive disaster scenario. The recovery plan should include a hot site in a different building complex and storage of back-up tapes at an off-site secured facility a reasonable distance from the legislative buildings. This would reduce the likelihood that a disaster would affect both the primary processing site and the off-site storage location. New procedures and an agreement for a hot site will need to be put in place to support the new scenario. Furthermore, the disaster procedures will need to be tested periodically.

Finding 134 - LASD does not manage the computer room as a closed shop.

Currently any LASD staff can gain access to the computer room. This is primarily for access to the computer printer and plotter (i.e., redistricting).

Recommendation - Make the computer room a closed shop.

Open access to the computer room constitutes an unnecessary security exposure. As soon as the redistricting project is completed, the computer room should be made a closed shop operation. The only individuals who have a regular need to enter the computer room are the operator and systems programmer, and occasionally the manager. Computer listings can be removed from the computer room and placed outside for pick up.

Finding 135 - LASD does not use its budget as a management tool.

No budget or actual expenditure information is available for LASD, not even for the manager. Another office in the Legislative Administrative Office was the only source for this information.

Recommendation - LASD should have an explicit operating budget.

LASD should know and have available both its operating budget and actual expenditures. Otherwise the manager is not in a position to make expenditure decisions or to monitor the financial status of his operation. The automated systems budget should be used as a planning and management tool to operate the organization.

Finding 136 - LASD job descriptions are not current.

The documents provided as job descriptions are not in fact current job descriptions, but descriptions used in the job recruitment process that took place five or more years ago. They have not been updated in a number of years, and at least one needs significant update. The job descriptions contain only information concerning what generally needs to be performed, and contain no performance measures.

Recommendation - LASD job descriptions should be updated to reflect the current roles and responsibilities.

The job description should not read like a recruiting ad. It should contain quantitative measures of performance against which the employee can be measured.